vmware® airwatch®

VMware AirWatch Guide for the Apple Device Enrollment Program (DEP)

Using Apple's DEP to automatically enroll new devices with AirWatch MDM

Workspace ONE UEM v9.4

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to Apple DEP Integration

To maximize the benefits of Apple devices enrolled in Mobile Device Management (MDM), Apple has introduced the Device Enrollment Program (DEP). With DEP, you can perform the following.

- Install a non-removable MDM profile on a device, preventing end users from being able to delete it.

- Provision devices in Supervised mode (iOS only). Devices in Supervised mode can access additional security and configuration settings.

- Enforce an enrollment for all end users.

- Meet your organization's needs by customizing and streamline the enrollment process.

- Prevent iCloud back up by disabling users from signing in with their Apple ID when generating a DEP profile.

- Force OS updates for all end users.

> **Disclaimer:** Integration with any third-party software product is not guaranteed, and is dependent upon the proper functioning of those third-party solutions.

DEP Security Features

Devices managed by Workspace ONE UEM and enrolled through the Apple Device Enrollment Program can receive security measures to protect end-user and corporate data when a device is lost or stolen.

Maximum App Passcode Attempts

You can configure your DEP devices to require the end user to enter a passcode to access SDK apps on the device. You can also set a maximum number of attempts to enter the passcode correctly. If this feature is enabled, and a user exceeds the maximum device passcode attempts, the device locks into Lost Mode. A device in Lost Mode can only be unlocked from the UEM console.

To configure the app passcode settings, navigate to **Groups & Settings > All Settings > Apps > Security Policies** in the UEM console.

For more information, see Complete the DEP Enrollment Profile on page 14.

Agent Unenroll Protection

If an end user attempts to unenroll a supervised DEP device through the AirWatch Agent, the device locks into Lost Mode. A device in Lost Mode can only be unlocked from the UEM console.

For more information, see Perform Remote Actions on All Devices on page 24.

Apple DEP Integration Prerequisites

To integrate with the Device Enrollment Program, you must complete the following requirements.

- **An Apple DEP account** – Register for a DEP account. If needed, enroll with Apple using the Apple [Enrollment Procedure](#).

- **Apple devices** – Any macOS, iOS, and tvOS devices that you want managed through DEP must be associated with a DEP account.

  - Devices purchased from a Third party or reseller must be associated with your DEP account. To make sure that the devices are DEP-eligible, check with your reseller.

  - When enrolling devices, you must have Internet connectivity.

- When integrating with the Apple DEP portal, ensure that the network is set up to communicate with **mdmenrollment.apple.com** on port **443**, as for some on-premise clients.

Chapter 2:
Device Enrollment

DEP Device Enrollment

Using a registered device, follow the standard iOS Setup Assistant process, including language, country or region, and Wi-Fi network. From this point, the Setup Assistant flow is determined by settings in the DEP profile that was assigned to the device.

The Setup Assistant will not show features that you decided to skip. It only shows screens related to what you choose not to skip.

Once automatic configuration and enrollment is complete, the Setup Assistant closes and the device is ready for use with the Workspace ONE UEM MDM profile and settings provisioned onto the device.

For iOS devices enrolled using Apple's Device Enrollment Program (DEP), enrollment restrictions do not apply. This is because device information such as OS version, device model and more is only received after the device has been enrolled through DEP.

Enroll Apple Devices using Apple DEP

Since the device is registered with the Apple Device Enrollment Program, follow the Setup Assistant on the device to complete DEP enrollment. The Setup Assistant displays the options that were chosen when the DEP profile was created for that device.

If you require end users to generate their own enrollment tokens in the Self-Service Portal, they must complete that step before enrolling their devices. For more information about end-user generated tokens, see Alternate DEP Device Enrollment Flows on page 10.

To enroll a DEP-enabled device:

1. When the device is connected to wifi, log in to the device with the end-user enrollment credentials. You will see the additional Workspace ONE UEM MDM configuration prompt.

2. Complete the steps in the Setup Assistant.

3. Verify that Supervised status is enabled by navigating to **Settings > General > About** on the device. Under the Device Name you will see a notification that the device is Supervised.

4. Verify that the MDM profile is not removable by navigating to **Settings > General > Profiles** and selecting the Workspace ONE UEM MDM profile. You will see there is no option in the form of an icon to remove the profile.

For more information on DEP Enrollment for tvOS devices and macOS devices, see **VMware Workspace ONE UEM Apple tvOS Platform Guide** and **VMware Workspace ONE UEM macOS Platform Guide**.

Enable Registration Tokens for DEP Enrollment

If you restrict enrollment to registered devices only, you also have the option of requiring a registration token. This option increases security by confirming that a particular user is authorized to enroll.

To enable token-based enrollment:

1. Select the appropriate organization group and navigate to **Devices > Device Settings > Devices & Users > General > Enrollment** and ensure the **Authentication** tab is selected.

    Scroll down past the **Getting Started** section and select **Registered Devices Only** as the **Devices Enrollment Mode**. A

checkbox labeled **Require Registration Token** will appear in which you should insert a check mark. This will restrict enrollment to only registered devices.

Authentication Mode(s)	☑ Basic ☑ Directory ☐ Authentication Proxy
Devices Enrollment Mode *	○ Open Enrollment ◉ Registered Devices Only
Require Registration Token	**ENABLED** DISABLED
Registration Token Type *	◉ Single-Factor ○ Two-Factor
Registration Token Length *	6 ⓘ
Token Expiration Time (hours) *	24

2. Select a **Registration Token Type**.

   • **Single-Factor** – The token is all that is needed to enroll.

3. Set the **Registration Token Length**. This required field denotes how complex the Registration Token is and must contain a value between 6 to 20 alphanumeric characters in length.

4. While you can set the **Token Expiration Time** (in hours), note that it does not apply to DEP devices at this time.

Alternative methods for generating an enrollment token exist. For more information, see Alternate DEP Device Enrollment Flows on page 10.

Specify Enrollment Token Delivery Method

1. Navigate to **Accounts > Users > List View** and select **Edit User** for a user. (This process also works with creating new users.) The Add / Edit User page displays.

2. Scroll down and select a **Message Type: Email** for directory users and **SMS** for basic user accounts.

Generate Enrollment Token

Once the MDM profile is installed on the device, the token is considered "used" and cannot be used to enroll other devices. If enrollment was not completed, the token can still be used on another device.

DEP Profile Settings for Token Enrollment

Use a DEP profile with **Authentication** set to **On** to prompt the user to enter credentials – a username and password – during the Setup Assistant process. If **Require Registration** with a **Single-Factor** token is enabled for the organization group which has DEP configured, the user must enter the one-time token that is sent to them into both the username and password fields.

For better user experience – and to direct users to follow the process – consider creating a custom message template, which can have a message similar to: "Please enter the one-time token you received through email or SMS into both the username and password fields."

Generate a DEP Token

A DEP token allows your end users to enroll their devices simply and securely.

To generate a DEP token:

1. In the Workspace ONE UEM console, navigate to Add > Batch Import.

2. Select Batch type **Users And/Or Devices**. You may chose to use a Simple Template or Advanced Template depending on your need.

3. To generate a Token, map an enrollment user to DEP device serial number. This will generate a token and deliver it to the user according to their preferred method of notification, which is specified under User Settings.

Alternate DEP Device Enrollment Flows

Combining the functionalities of the Apple DEP portal and the AirWatch Self-Service Portal, administrators can enable alternate end-user enrollment flows.

Alternate enrollment flows:

- The end users generate their own enrollment tokens in the AirWatch Self-Service Portal.
  - To enable this option, you must have the Self-Service Portal enabled for your end users.
  - The generated token is valid for the expiration time set in Token Enrollment settings in the Admin Portal.
- The administrator generates an enrollment token in the UEM Console without entering a device serial number.
  - Either the admin or the end user can enroll the device with the generated DEP token, which is configured and sent in the usual way.
  - The generated token is valid for the expiration time set in Token Enrollment settings in the Admin Portal.
  - An advantage of this enrollment flow is that neither admins nor end users are required to enter the device serial number during enrollment. This function is useful in deployments where devices are not preassigned to users, such as in a school setting.
- The administrator generates an enrollment token using the bulk upload option in the Workspace ONE UEM Admin Console, specifying the device serial number.
  - Either the admin or the end user enrolls the device using the generated DEP token, which is configured and sent in the usual way.
  - A token generated using the Bulk Upload method has no expiration date.
  - For more information about uploading device serial numbers in bulk, see Associate Devices in Apple's DEP Portal on page 19.

Perform DEP Enrollment with a Registration Token

Once you have sent the Registration Token to the end user, perform the enrollment on the device.

To perform the enrollment with a registration token:

1. Turn on the DEP device.

2. Complete the setup screens as part of the Setup Assistant.

   For more information on these settings, see Complete the DEP Enrollment Profile on page 14

3. On the authentication screen that requires a username and password, the user must enter the token they received into both the username and password fields. The end user must enter the same token information under both Username and Password. To keep the end user informed you can define the message that will be shown on the authentication screen to direct the user to enter the token under both username and password.

   For more information, see Enable Registration Tokens for DEP Enrollment on page 8.

View DEP Device Enrollment Status

Check the enrollment status of your devices to view DEP-specific information, and generate reports when needed.

1. Navigate to **Devices > Lifecycle > Enrollment Status**.

2. In addition, DEP-specific devices can have one of the following **Enrollment** statuses:

   - **Discovered** – Devices that are synced into Workspace ONE UEM but are not assigned a DEP Profile. These devices would not receive the MDM enrollment prompt during the Setup Assistant.

   - **Registered** – Devices are assigned a DEP Profile and you will see the MDM enrollment prompt during the Setup Assistant.

   - **Enrolled** – Devices are enrolled into Workspace ONE UEM MDM and can now be managed from the **Devices > List View** page.

3. Go to **Layout** and make column selections to view specific information about enrolled devices.

   - **Serial Number** – Device's unique serial tracking number.

   - **Asset Number** – Internally allocated device tracking number.

   - **Profile** – DEP profile assigned to the device.

   - **Department** – Department attached to the DEP profile assigned to the device.

   - **Source** – Designates whether the device is associated with the Device Enrollment Program.

Chapter 3:
Integration with Apple's Device Enrollment Program

Apple DEP Integration Overview

Integrating with Apple's Device Enrollment Program (DEP) requires completing tasks in both the UEM console and in Apple's DEP portal.

Your organization must already be registered with Apple's Deployment Programs. During the integration, Workspace ONE UEM recommends that you do not use Internet Explorer as your browser. Also, once you begin configuring the DEP wizard in the UEM console, keep the browser session open. You cannot save your activity until you complete the final configuration step, so it is important to finish the entire configuration in one browser session.

Set Up the Apple DEP Portal

Start in the UEM console to begin integrating your Workspace ONE UEM deployment with DEP. Then move to the Apple DEP portal to create a virtual MDM server container for your organization's devices.

For more information, see Download the Public Key to Integrate with Apple DEP on page 13.

Configure Devices and the DEP Portal

Next, configure your devices and the UEM console to create an initial profile.

For more information, see Configure the Apple DEP Portal on page 13.

Assign and Manage Devices

Finally, assign devices to the virtual MDM container in Apple's portal, so they can be managed through Workspace ONE UEM.

For more information, see Associate Devices in Apple's DEP Portal on page 19.

Download the Public Key to Integrate with Apple DEP

Begin integrating with the Apple DEP program by downloading a public key (.pem) that allows Workspace ONE UEM and Apple to mutually authenticate with each other in order to sync devices. This key is uploaded to the Apple portal later.

1. Log into the UEM console and navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program** and select **Configure**. A **Device Enrollment Program** window appears.

2. Download the public key by selecting the **MDM_DEP_PublicKey.pem** file.

3. Save the public key in a convenient location. This is used to complete the DEP setup process.

Using the public key you have downloaded, you must next enable and configure the Apple DEP Portal so you can manage your DEP-enrolled devices in the Workspace ONE UEM Admin Console.

Configure the Apple DEP Portal

Create a virtual MDM server for devices that links to your own MDM servers, so you can manage devices directly in the UEM console. Workspace ONE UEM does not recommend using Internet Explorer to complete this process.

Before you begin to configure the DEP Portal, you must have your downloaded public key. For more information, see Download the Public Key to Integrate with Apple DEP on page 13. When you have you public key, perform the following steps.

1. Select the Apple Deployment Programs link in the **Device Enrollment Program** window to be directed to Apple's website. Do not close this browser session. You will navigate back to this window after completing the DEP enrollment process below.

2. Sign in with your organization's Apple credentials.

3. Select **Get Started** to automate MDM enrollment.

4. Confirm your identity by entering the verification code. The Device Enrollment Program portal screen appears.

5. Select **Manage Servers** in the left-navigation pane.

6. Select **Add MDM Server** to create a container that groups devices in the DEP portal for management in the UEM console. The MDM server name may refer to a server, department or location.

7. Enter the **MDM Server name** for your organization. Select **Next**.

   If you choose the next option and select **Automatically Assign New Devices**, then each device (determined by serial number or purchase number) that is added to your DEP account from this point forward is automatically associated with that MDM server.

8. Select **Upload File** and **Upload your Public Key**. Navigate to the MDM_DEP_PublicKey.pem that you downloaded from the UEM console earlier and upload it. Select **Next**.

9. Select **Your Server Token** to receive an encrypted Apple Server Token file (.p7m) and save it in a convenient location.

10. Select **Done**.

DEP Profile Creation

After assigning devices to the DEP portal, use the Device Enrollment Program wizard in the Workspace ONE UEM console to create an initial DEP profile to configure authentication, MDM features and the Setup Assistant to push down to devices.

You must assign this DEP profile prior to configuring the device's Setup Assistant that appears after you power the device on for the first time. Devices only reach out to Apple's server once after configuring Wi-Fi to receive the DEP profile. If the correct DEP profile is not assigned to the device prior to Wi-Fi configuration, a factory wipe is required (using iTunes or directly on the device).

Complete the DEP Enrollment Profile

After you register devices with Apple, use the Workspace ONE UEM DEP profile wizard to create a DEP enrollment profile. An enrollment profile is a collection of DEP settings assigned to your registered devices. You can create more profiles later if needed.

Create a new DEP enrollment profile or edit an existing profile.

1. In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.

2. Select **Upload** and select Apple Server Token File (.p7m). Select **Next**. Now Workspace ONE UEM and Apple can authenticate each other. For more information on tokens, see Best Practices for Adding Tokens.

For clarity, use only one token at the customer organization group. Only add multiple tokens if your organization has a complex configuration, or if you are enrolling devices with multiple DEP accounts.

3. Configure the **Authentication** settings, based on whether you turn authentication **On** or **Off**. Authentication settings are only available for devices running iOS 7.1 and higher. If devices running iOS 7.0 and lower are assigned an authentication profile, the devices are automatically enrolled using staging authentication.

- If you turn on **Authentication**, each user must tie a DEP device to their own user account.

- If you turn off **Authentication**, you can enable staging of all devices under a single user account, and extra configuration options appear on the Settings page to accommodate this option.

If you set Authentication to **On**, then configure:

Setting	Description
Device Ownership Type	Determines the ownership type of the device upon enrollment, which can be either Corporate-Dedicated, Corporate-Shared, or Employee-Owned.
Device Organization Group	Select the organization group your where your end users authenticate. Only end-user accounts created at this level or a parent above it can authenticate their devices. End users may authenticate using either their Active Directory credentials or basic Workspace ONE UEM credentials, depending on which authentication type you have enabled under Enrollment settings.
Custom Prompt	Turn **On** Custom Prompt to enable custom text to appear on the device authentication screen during the Setup Assistant. Authentication occurs when end users are prompted for their credentials. For Apple School Manager, turn **Off** Custom Prompt if you are deploying shared iPads.
Message Template	Choose a message template to send as a Custom Prompt. (Supported for English-language only.) This option is not available when **Custom Prompt** is **Off**.

If you turn Authentication **Off**, then configure:

Setting	Description
Default Staging User	Select the Enrollment User assigned to the device.
Device Ownership Type	Select the ownership type of the device upon enrollment, which can be either Corporate-Dedicated, Corporate-Shared, or Employee-Owned.
Device Organization Group	Select the organization group where your devices are enrolled.

4. Configure **MDM features** of the device.

Setting	Description
Profile Name	Enter the name of the profile as it appears in the UEM console.

Setting	Description
Department	Enter the name of your department as it appears in the device's **About Configuration** panel upon setup and enrollment.
Support Number	Enter your organizational support contact phone number as it appears in the device's **About Configuration** panel upon setup and enrollment.
Require MDM Enrollment	Select **Enable** to require end users to enroll into Workspace ONE UEM MDM. Use this setting to ensure end-user devices cannot be activated unless they enroll into Workspace ONE UEM MDM.
Supervision	Enable to set the device in Supervised mode, which is an alternative to configuring Supervised devices using Apple Configurator. Supervision is required for shared devices.
Shared Devices	Enable this option to use shared devices with education functionality. This option must be enabled for shared devices using Apple School Manager.
Lock MDM Profile	Select **Enable** to prevent end users from unenrolling from Workspace ONE UEM MDM. This setting ensures that end users cannot remove the Workspace ONE UEM MDM profile installed on the device. This option may only be enabled if Supervision is enabled.
Anchor Certificate	Enable this option to upload certificates as trusted anchor certificate and push to devices during DEP enrollment. These certificates are used as trusted anchor certificates when evaluating the trust of the connection to the MDM server URL. If no certificate is uploaded, the built-in root certificates will be used.
Device pairing	Enable to allow the device to sync with any workstation through iTunes, Configurator, and iPCU. Optionally, set Device Pairing to **Disable** when deploying education functionality, and **Upload** a **Device Pairing Certificate** for supervised identities. From Workspace ONE UEM 9.2.2, you can upload Device Pairing Certificates whether Device Pairing is set to Enabled or Disabled.
Await Configuration	Enable this setting if the MDM server is expected to send extra commands before the device can allow the user to proceed in the Setup Assistant. Await Configuration is required for education functionality. To override the Await Configuration setting on a device, navigate to **Device > Details View** and select the device to override. Select **More Actions > Device Configured** to note the device as configured and skip the Awaiting Configuration screen during enrollment. If you enable **Await Configuration**, more options appear in the **Setup Assistant** section.
Auto Advance Setup	Enable this setting to automatically apply DEP configuration to an enrolling device. Users can skip all setup panes, and the device is automatically set to the most restrictive option by default within around 30 seconds after network active. Applies to ethernet-connected tvOS devices only.

5. Choose the items seen by end users during the Apple **Setup Assistant** workflow that appears after the device is powered on for the first time. For Apple School Manager, **Skip** all Setup Assistant options.

Setting	Description
Passcode	Select **Don't Skip** to require user to set a passcode during setup. If an MDM passcode profile is already set up through Workspace ONE UEM, select **Skip**.
Touch ID	Select **Don't Skip** to prompt user to configure Touch ID during setup.
Location Services	Select **Don't Skip** to prompt user to enable or disable Location Services during setup. If you plan on tracking GPS locations for your devices, select **Don't Skip**.
Restoring from Backup	Select **Don't Skip** to prompt user to restore from backup during setup. You must select **Don't Skip** to allow users to move data from a previous device, including an Android Device.
Move from Android	If **Restoring from Backup** is set to **Don't Skip**, select **Don't Skip** in this pane to prompt users to move accounts and data from an Android device during setup.
Sign in with Apple ID and iCloud	Select **Don't Skip** to prompt user to sign in with an Apple ID and iCloud account during setup.
Terms of Use and Conditions	Select **Don't Skip** to prompt users to read and accept the Terms of Use and Conditions during setup.
Siri	Select **Don't Skip** to prompt user to configure Siri. If you select **Skip**, Siri is disabled on enrolled devices.
Diagnostics	Select **Don't Skip** to prompt user to enable or disable sending diagnostic data to Apple. If you select **Skip**, sending diagnostic data is disabled on enrolled devices.
Registration	Select **Don't Skip** to prompt user to register the device with Apple during setup.
Apple Pay	Select **Don't Skip** to prompt user to set up an Apple Pay account during setup. If you select **Skip**, Apple Pay is disabled on enrolled devices.
Zoom	Select **Don't Skip** to prompt user to enable zoom functionality during setup.
FileVault 2	Select **Don't Skip** to prompt user to set up a FileVault account.
Display Tone	Select **Skip** to allow users to skip the display tone setup step for enrolling iOS devices.
Home Button Sensitivity	Select **Skip** to allow users to enroll devices without configuring the Home button sensitivity on enrolling iOS devices.
Tap to Setup	Select **Skip** to allow enrolling tvOS devices to enroll without an associated iOS device.
Screen Saver	Select **Skip** to allow users to enroll a tvOS device without configuring a screen saver.
Keyboard	Select **Skip** to omit the prompt for users to select a keyboard type during the Setup Assistant process.
Onboarding	Select **Skip** to prevent users from viewing on-boarding informational screens for user education during the Setup Assistant process.
Watch Migration	Set to **Skip** to prevent users from viewing options for watch migration during the Setup Assistant process.
iCloud Analytics	Set to **Skip** to omit a user prompt to send analytics to iCloud during setup.

Setting	Description
iCloud Documents and Desktop	Set to **Skip** to prevent users from viewing iCloud Documents and Desktop screen in macOS.
TV Home Screen Sync	Set to **Skip** to prevent users from toggling the TV home screen layout during setup.
TV Provider Sign In	Set to **Skip** to prevent users from signing in to a TV provider during setup.
Where is the Apple TV?	Set to **Skip** to omit the **Where is this Apple TV** screen on tvOS devices enrolling through DEP.
Privacy	Set to **Skip** to omit the **Privacy** screen in DEP setup assistant while onboarding.

6. For certain configurations detailed in the **Setup Assistant** configuration, use the **Admin Account Creation** section to create an admin account for local and remote macOS device admin actions.

Setting	Description
Account Setup	This item appears only if **Await Configuration** is set to **Enabled**. Select **Don't Skip** to require users to create an account during setup. Configure the type of account the user creates in **Account Type**. Select **Skip** if you have created a Directory Profile for the user and they do not need to create an account. Configure the admin account for this selection in the **Admin Account Creation** section.
Account Type	This item appears only if **Account Setup** is set to **Don't Skip**. Select **Standard** to give users access to a standard user account on their macOS device. If you select Standard, you must create an admin account to manage the Standard account. Select **Administrator** to allow users to create an Administrator account on their macOS device.
Password	Create a password for the admin account.
Hidden	Select **Enabled** to hide the admin account on the macOS device. Hidden admin accounts can enhance security and user experience. Select **Disabled** to make the admin account visible when a user logs in.

7. Select **Save** to view the **Summary** page and review the settings you have selected. Assign the settings to devices registered in the Device Enrollment Program.

Setting	Description
Sync Now and Assign to All Devices	Select **Yes** to save and deploy the DEP profile settings to all devices that are currently registered with the MDM server that you just created in the DEP portal. Selecting **No** saves the DEP profile settings but does not deploy them to devices. You can sync and assign the DEP profile at any time.

Setting	Description
Auto Assign Default Profile	Select **Yes** to push the DEP profile settings to all devices that are currently registered once they are synced with Workspace ONE UEM **and** any devices from that point on as they are newly registered with Apple and synced with Workspace ONE UEM.
	Selecting **No** means newly-registered devices do not automatically receive the DEP profile settings. Enable this setting if you plan to create multiple DEP profiles for different devices.

8. Once the deployment options are configured, select **Save**. You are now ready to manage profiles on DEP-enabled devices from the UEM console.

Associate Devices in Apple's DEP Portal

Associate devices with the MDM server in the DEP portal so that they can be synced and managed with Workspace ONE UEM. You can assign additional devices at a later time using these same steps, if required.

1. Navigate to Apple's Device Enrollment Program portal.

2. Select **Device Enrollment Program > Manage Devices** in the left panel to assign DEP-enabled devices to the MDM Server you already created.

3. Select the method for associating devices and **Choose Devices By**:

   - **Assign Devices by Serial Number** – You can enter a list of device serial numbers.

   - **Assign Devices by Order Number** – You can enter your Apple Purchase Order number and have devices added automatically.

   - **Upload a .csv File** – Upload a .csv file listing the serial numbers.

4. Choose **Assign to Server** as the **Action** and select the MDM server group.

5. Select **OK**.

Disassociate Devices in the Apple DEP Portal

If necessary, you can manually disassociate a device from the Device Enrollment Program. Do this if the device was lost or stolen.

1. Return to the DEP portal and manually disassociate it from the MDM server that you initially created.

2. Delete device records using Delete DEP Device Records on page 25.

3. Sync the devices in the UEM console using Sync Apple DEP Devices Manually on page 23.

The device record no longer appears on the Enrollment Status page or in the List View.

Chapter 4:
Device Enrollment Program Profile Management

Create Additional DEP Profiles

After the first DEP profile is initially created, create profiles quickly without having to return to the DEP wizard. This allows you to create multiple profiles to use for different deployments.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**. Since you already configured a DEP profile using the Workspace ONE UEM Setup Wizard, a new screen displays.

2. Select **Add Profile**.

3. Configure the settings for a new DEP profile, as described when using when using the profile wizard earlier.

4. **Save** the profile. This profile is added to the list of other profiles.

5. From the **Default Profile Assigned for Newly Synced Devices** menu, select the DEP profile you want to automatically assign to all devices upon being synced into Workspace ONE UEM. If you do not wish to push a DEP profile to new devices, select **None**.

Edit an Existing DEP Profile

Modify existing DEP profiles to more closely meet the needs of your organization or deployment.

To edit an existing DEP profile:

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**. The DEP profiles you have already created appear.

2. Select the **pencil icon** to edit the profile. The **Edit Profile** window appears.

3. Edit the DEP profile settings from this window. Settings are not applied until the changes register during the Setup Assistant.

4. Select **Save**.

Manually Assign or Remove a DEP Profile

Depending on the DEP profile settings you selected, the DEP profile is assigned automatically or you may choose to manually assign it.

For Apple School Manager deployments, you must assign profiles to the appropriate devices after creating them for both Shared iPad and one-to-one configurations.

1. Navigate to **Devices > Lifecycle > Enrollment Status.**

2. Select the devices needed for the action.

3. Select the **More Actions > DEP Profile** and select one of the following options:

   - **Assign Profile** – Assign new or additional DEP profiles to selected devices. The DEP profile is not updated on a device until the device is factory wiped or re-connected to Wi-Fi.

   - **Remove Profile** – Removes existing DEP profiles from selected devices.

Chapter 5:
Device Management

Sync Apple DEP Devices Manually

Before you can manage any DEP-enabled devices you must sync them from the UEM console after you register them with Apple.

> **Note:** If you selected **Sync Now and Assign to All Devices**, then the registered devices are automatically synced when you save your DEP Profile. If you decide to add more devices later, perform a manual sync using the instructions below or wait for the DEP sync scheduler to run.

1. Navigate to **Devices > Lifecycle > Enrollment Status.**

2. Select the devices to sync.

3. Navigate to **Add > Sync Devices** and follow the prompt to complete the process.

   - **Sync Devices** – Selecting this option populates the UEM console with any newly registered devices from Apple's Deployment Programs. It also automatically assigns the current **Auto Assign Default Profile** to devices, if the feature was configured earlier.

Use the DEP Sync Scheduler

While a manual sync can be issued at any time, Workspace ONE UEM syncs with DEP-enrolled devices every 24 hours. Configure the sync schedule by accessing the DEP Scheduler in the UEM console. The schedule setting is only available to System Administrators at the Global organization group level.

1. Navigate to **Groups & Settings > All Settings > Admin > Scheduler.**

2. Select **Add Schedule > Device Enrollment Program Updates**.

3. Create a name and description for the **task**.

4. Determine the **recurrence type**.

5. Determine the range for the schedule.

6. Select **Save** to add this schedule to the list.

Renew Your Apple Server Token for DEP Deployments

Your Apple Server Token file is valid for one year, after which time you must renew it.

1. Log into the Apple Deployment Programs site and select **Get Started** for the Device Enrollment Program.

2. Confirm your identity with a verification code by selecting the phone number to receive the four-digit code and select **Send**. When received, enter the code. Select **Continue**.

3. Select **Manage Servers** from the left panel.

4. Select the **Server Name** of your MDM server with the token file you want to renew.

5. Select **Generate New Token > Generate and Download Server Token**.

6. Select **Done > OK**.

7. Navigate to the DEP settings page in the UEM console.

8. Go to **Groups & Settings > All Settings > Devices & Users > Apple > Device Enrollment Program**.

9. Select the **Renew** button.

TOKEN

Token Name   Q___ @ _Token_ @ _____

Expiration Date   3/23/2017 2:04:29 PM

[Renew]   [Fetch All Devices]

10. Upload your newly generated server token.

Best Practices for Using Tokens

Administrators can add DEP profiles or upload tokens at any organization group, even in a child organization group.

- Add DEP profiles to all devices that are registered to that organization group by specifying the token name when adding the profile.

- Administrators can override permissions in a child organization group and add multiple tokens to any group inheriting the DEP configuration.

Best Practices for using Fetch to Sync Devices

Fetch syncs all the Device Enrollment Program devices with the UEM console, including devices that may were already synced. It should only be used when devices are not syncing. Workspace ONE UEM recommends Fetch as a final alternative in this case.

Generate DEP Reports

You can automatically or manually generate reports in the UEM console to keep track of DEP-associated devices.

1. Navigate to **Hub > Reports & Analytics > Reports > List View**.

2. Access the **Device MDM Detail** report.

3. Complete the form and select **Download**.

Perform Remote Actions on All Devices

Select a device or group of devices to complete the following actions.

1. Navigate to **Devices > List View > Select Device.** The **Details View** appears.

2. Select **More Actions** and choose from the following education-specific actions.

   - **User Lists (Query)** - Send a query command to the device to return a list of cached users.

   - **Device Configured (Admin)** - Send this command if a device is stuck in an Awaiting Configuration state.

   - **Log out user (Admin)** - Log out the current user of the device if needed.

   - **iOS updates (Admin)** - Select individual devices or devices in bulk to update devices.

   - **Enable/Disable Lost Mode** – Lock a device and send a message, phone number, or text to the lock screen. Lost Mode is disabled by administrators only. When Lost Mode is disabled, the device returns to normal functionality. Users are sent a message that tells them that the location of the device was shared.

     - **Request Device Location** – Query a device in Lost Mode, and then access the Location tab to find the device. (iOS 9.3 + Supervised)

Delete DEP Device Records

You can remove DEP-enabled device records from the Device List View in the UEM console for enrolled devices while the device remains registered with the Device Enrollment Program.

Once this device record is deleted, the device status changes from enrolled to unenrolled. Simply factory wipe the device and re-enroll it.

1. Navigate to **Devices > List View.**

2. Select the device(s) to delete.

3. Navigate to the **More** drop-down menu.

4. Select **Admin > Delete**.

> **Note:** The UEM console only allows you to delete a device record. You will be prevented from manually deleting a DEP-enabled device here. See Disassociate Devices in the Apple DEP Portal on page 19 sto manually delete a device the Device Enrollment Program.

Wiping DEP-enrolled Devices

You should not perform an enterprise wipe through Workspace ONE UEM on an enrolled DEP device. Instead, perform a device wipe, so the user is forced to re-enroll when it is reactivated. To discourage an enterprise wipe on DEP devices, Workspace ONE UEM displays an additional warning in the UEM console when performing the command.

Additionally, Workspace ONE UEM recommends restricting the Self-Service Portal (SSP) role for end users from using the device wipe command. You can configure these roles by navigating to **Accounts > Users > Roles**.